DEFENSE INFORMATION SYSTEMS AGENCY
CUSTOMER ADVOCACY

April 2002
Volume 2, Number 1

Customer Connection

The Voice for the Warfighter

Inside This Issue

The Customer Connection is published quarterly under the auspices of Customer Advocacy to provide readers with relevant information about DISA products and services. Articles printed herein are for informational purposes only, and do not represent official DISA policy, and views and opinions expressed are those of the authors. The mention of commercial products and/or services does not imply endorsement by the Department of Defense or the Defense Information Systems Agency.

Defense Information Systems Agency
Customer Advocacy
701 South Courthouse Road
Arlington, VA 22204-2199

From The Director

We're pleased to present you with the 2nd edition of DISA's *Customer Connection* as part of our continuing effort to provide the latest information on DISA products and services, customer issues, and DISA initiatives. This quarter, we are highlighting DISA's Computing Services Directorate. We are very proud of these services and I believe you will be impressed with what we offer to improve your mission at a reasonable cost.

You will also find articles on several other key areas of interest. We have included information about the new DISA Customer Partnership Conference in July. We also present articles on Acquisition services that describe the critical support that dedicated DISA professionals offer, the new Senior Executive Account Manager (SEAM) Partnership Program that provides additional customer focus, and DISA's Customized Status Reporting.

I was recently honored to host each of the Service Secretaries. We had very informative and productive sessions, and I believe they all came away with a better understanding and appreciation of what DISA can do for their organizations. There is an excellent article in this issue on these meetings.

Our goal is to make DISA a world-class leader in supplying information services to our customers and providing exceptional customer support. Please let us know what we can do to serve you better.

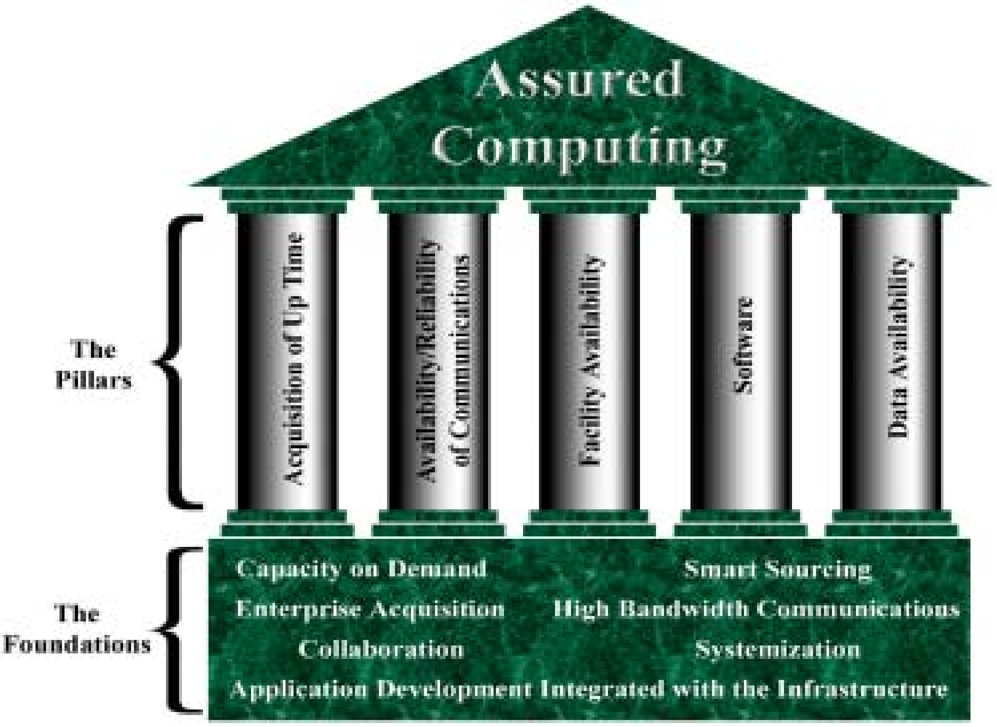
May God Continue to Bless America.

Assured Computing Implemented for Unisys Processing

By Shelley Madden

The DISA Computing Services' implementation of assured computing in the Unisys mainframe environment during December 2001 is a first for the federal government, and a first in the industry in scope and complexity. Assured computing is a set of initiatives designed to ensure information and mission critical applications are always available to customers. It addresses the demand for nondisruptive data availability, while providing significant improvements in the reliability and scalability of information supporting the warfighter. DISA has been pursuing this computing concept for nearly three years, and the need for it was highlighted by the events of September 11.

DISA's implementation of assured computing was driven by the warfighter's need for information availability. Information technology is no longer a support function – it is a critical warfighter asset that must be continuously available. In the commercial world, "24x7" access is already standard practice for many wholesale and retail businesses, and it is widespread in the world of e-commerce. DoD is a "24x7" enterprise. For example, Air Force and Defense Finance and Accounting Services (DFAS) processing in a Unisys environment cannot operate under what was the conventional paradigm that permitted up to 72 hours of lag time between loss of computing capability and full restoration of service.



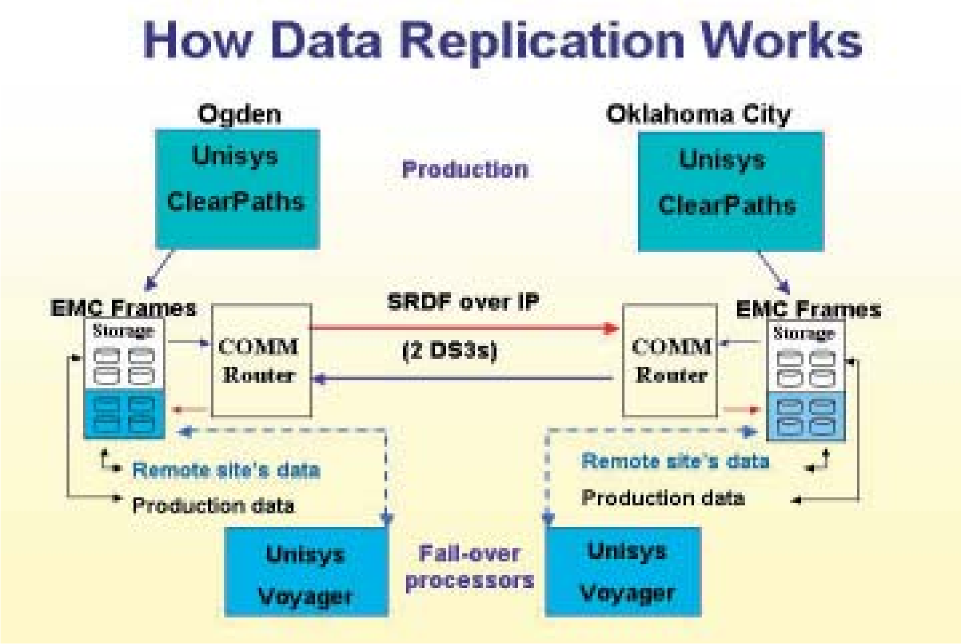
The five pillars of Assured Computing and its foundations.

Capital investment in facilities has significantly reduced facility-related outages. Consolidated hardware maintenance contracts are in place to increase system uptime. A robust architecture and infrastructure, with redundant elements in place, substantially reduces the possibility that loss of any component could disable an entire site. Assured computing also includes measures to enhance data availability, including the use of remote data replication and mirroring at geographically separate locations. These latter techniques will blunt the effects of a catastrophic event, such as loss of one site or major system, which could cripple warfighter support or supporting business processes.

Assured computing for the Unisys mainframe environment became a reality in December 2001 when DISA implemented an innovative operating design for data replication and mirroring at the Defense Enterprise Computing Centers (DECC) in Oklahoma City and Ogden. In the new design, the operating system and storage subsystems work in tandem to create copies of all user data at routine intervals throughout a 24–hour day. This data replication, coupled with on demand mainframe processing power, gives DISA the unprecedented ability to relocate mainframe processing within hours when a catastrophic failure of processing support occurs.

The deployment of this new design and new technology created an environment in which the most essential component of the system, the data, is electronically stored at an alternate processing location. Appropriate processing capacity is built into each location so that disrupted service can be restored using the duplicate data available at the alternate site.

"For the past two years," said Air Force Lieutenant General Harry D. Raduege, Jr., Director of DISA, "we have made Defense Enterprise Computing Center availability, and the data we process a prior-



Billy Phillips, Unisys Technical Support, Shelley Madden, Enterprise Programs Division Chief, Cathie Netherton, Unisys Operating Systems Branch Chief, and Bob Torres, Lead PSI contractor, inspect state-of-the-art Unisys Voyager CPU which performs the Assured Computing data replication function.

ity: attacking single points of failure; ensuring that we acquired up time from our hardware vendors; and ensuring the data we process will be available even through a catastrophe. The latter includes this massive data replication effort for the Air Force and DFAS applications that run on Unisys mainframes at Oklahoma City and Ogden. Now, should a major facility failure occur at either place, the other would take the load," he added.

Planning and implementing data replication between Unisys mainframe computers at two DISA sites located more than 800 miles apart required a unique partnership of multiple commercial vendors and many elements of DISA. The team worked to resolve technical issues, solve logistics problems, and document the process for the benefit of the next assured computing initiatives. Building on two years of study, the team established an integration lab and initial prototype testing in early 2001. The testing duplicated in its entirety the Air Force Standard Base Level Computing environment and DFAS processing done at Oklahoma City and Ogden. The team declared success in February 2001 and, with proof of concept established, began the task of applying the concept in the more complex production world leading to completion last December.

How it works: Data is processed normally and captured on production storage Direct Access Storage Devices (DASD) disks. It is then duplicated and transferred across two DS 3 circuits that connect the sites. Each DS 3 follows a distinct route, so if one fails, the other picks up the traffic. The receiving site stores the alternate site's production data on the vendor provided DASD. The time required to accomplish a complete cycle of all production workload at both sites averages less than four hours. Data replication is a perpetual process; should a system or site fail, data loss would be minimized. The duplicate processing units are powered up but remain in an "idle" mode.

For additional information, contact Shelley Madden, CDK, (405) 734-4766, DSN 884.

Shelley Madden, Enterprise Programs Division Chief tries her hand at the Operations console for the new Assured Computing data replication equipment, while members of the Unisys staff look on.

The DISA Customer Partnership Conference - By Judy Naler-Fox

The DISA Customer Partnership Conference will be held July 30-31 at the Hilton Alexandria Mark Center, Alexandria, VA. This year, personal invitations will be extended to 400-500 customers and DISA staff. The theme of the conference will be "DoD Enterprise – Building the Vision...Together." The focus of the conference will be on issues and customers.

The agenda for the conference will include guest speakers, videos, and facilitated subconferences. Additional conference information will be disseminated in the near future and will also be available at the DISA website, www.disa.mil. For additional information, contact Judy Naler-Fox, CA1, (703) 882-0125, DSN 381.

Capacity on Demand Contracts - *By David Sloan*

The 21st century has brought new challenges for DISA Computing Services. Information technology continues to accelerate per Moore's Law: hardware tends to become obsolete in 12 to 18 months. Customers are demanding quicker responses to their dynamic requirements and they are not tolerant of downtime. As an IT service-provider, DISA has become more agile and flexible to meet these demands.

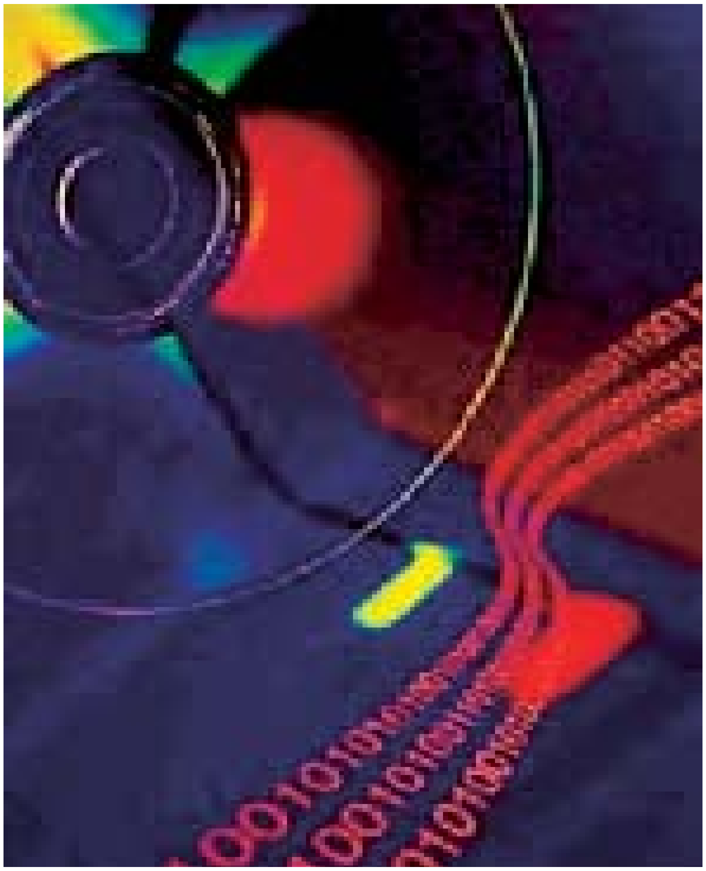
DISA Computing Services has three primary objectives in acquiring IT resources:

- Availability – meet the customers' needs for computing resources whenever needed.
- Military control – maintain confidence that the capability will not be compromised under crisis conditions.
- Cost – reduce DoD costs by acquiring only that processing capacity needed.

Traditional acquisition methods are not effective in meeting the responsiveness demanded by these objectives.

Our approach has shifted away from acquiring assets to acquiring services. While the commercial provider of these services will use hardware, software, and/or labor to perform, the contractual commitment is based strictly on usage. The service-provider sizes the capability to meet changing needs. Much like a homeowner pays for utilities by megawatt hours, BTUs, call minutes, or gallons consumed, we pay for computing resources by CPU-hours or gigabytes used. We require that the resources used to provide the services reside on our raised floor for full security and seamless integration within the Global Information Grid (GIG). But we are essentially paying only for the bits flowing out of those resources.

Computing Services has worked closely with private industry to establish capacity-on-demand utility-type contracts via GSA Schedules. We began awarding utility contracts for disk storage in February 2001. This is called Storage On Demand Services, or SODS.



Bits on Demand

Several of these contracts have been awarded for storage supporting midtier server requirements at DECC Ogden, and in August 2001, a contract was awarded for OS/390 mainframe storage at DECC Mechanicsburg and DECC Columbus. In addition, a contract was awarded in June 2001 for capacity-on-demand storage and processing services in support of our Unisys line of business at DECC Oklahoma City and DECC Ogden. Our first Processing On Demand Services (PODS) contract was awarded in January 2002 to supplant an OS/390 host at DECC Mechanicsburg.

In summary, DISA recognizes the need to react quickly to the requirements of our customers . We have acquisition vehicles in place, including a growing list of Blanket Purchase Agreements (BPAs), and we are anxious to work with our customers to take advantage of this new concept.

For additional information, contact David Sloan, Computing Services Acquisition Chief, at (703) 681-2266, DSN 761.

DISA Customized Status Reporting - *By Tim Phillips*

"What type of reports or metrics can you provide concerning network/circuit status or performance"? This is one of the most frequently asked questions the DISA Customer Advocates hear from customers.

There are many reports that provide situational awareness (SA) and keep the customer informed. Timely and accurate information not only keeps the customer informed, but it also provides a valuable tool for performance analysis and proactive customer service.

There are a number of standard daily reports promulgated by the DISA NIPRNet Network Operations Center (NOC) in Columbus that can assist in meeting customer's information requirements. Customer "Communications Reports" are provided for each of the military services and most agencies of the DoD. These reports are distributed daily via NIPRNet e-mail and include general information on major network outages that affect or have a potential impact on customers. A summary is also provided of the customer's open trouble tickets and a description of all trouble tickets closed since the last report.

Many customers have requested "high interest location" or activity status reporting, and the Columbus NOC Customer Advocate Teams (CAT) have developed a color-coded, stop-light type status report tailored for a customer's specific needs. These reports provide the customer with an easy-to-understand performance metrics usually over the last 24 hours. Another helpful report is the Network Health Trend Report which graphs bandwidth utilization, and helps the customer determine transmission speeds necessary to minimize circuit latency.

A new monthly performance report that details end-of-month metrics concerning circuit utilization, fault management, provisioning status, and trend analysis is being developed by the Columbus NOC. For information or to be added to the distribution list for any of the Columbus NOC reports, contact Mike Green at (614) 692-2058, DSN 850.

Another valuable report is the daily "DISA Morning Report" distributed via unclassified e-mail which provides a synopsis of the previous 24-hour Defense Enterprise Computing Center (DECC) status for availability, packet-loss, material release orders, and communications. A brief description of open trouble tickets is also provided (see example on page 10).

When there is a serious disruption or interruption of service affecting a DECC customer, a "High Interest DISA Alert" is sent via NIPRNet e-mail within one hour of the incident to all affected customers. These reports provide a detailed description of the "reason for outage" (RFO), and measures that have been taken to restore service. For information concerning these reports, contact the Shift Control Officer via e-mail at: rccrpt@crcc.disa.mil or call (614) 692-6348, DSN 850.

Keeping customers informed is one of DISA's goals, and these reports provide the customer the tools for up-to-date information. The next issue of the Customer Connection will provide information concerning new SIPRNet performance reports in development. POC for this article is Tim Phillips, CA3, (703) 882-2174, DSN 381.

Service Secretaries' Visits to DISA - *By Lt Col Bill McClure*

A critical part of the DISA transformation is "to put the customer first." One of the Director's initial actions in getting the word out was to invite the Service Secretaries to visit DISA. The Secretaries spent time with the Director and DISA's senior leadership, and discussed what the Agency does and how it can better service its customers as the Agency strives to become the DoD's preferred provider of information services.

The Secretary of the Navy, The Honorable Gordon R. England, visited DISA last August; Secretary of the Army, The Honorable Thomas E. White, visited in October; and Secretary of the Air Force, The Honorable James G. Roche, visited on 4 January. The Secretaries were briefed on how DISA and the National Communications System (NCS) are engaged on the "frontline" in the war against terrorism, and in supporting homeland defense. The Director highlighted accomplishments by DISA and NCS following the September 11th terrorist attacks. The Agency's senior leadership briefed the Secretaries on the Defense Information System Network (DISN); Computing Services initiatives; the fielding of warfighter decision superiority applications; and DISA's efforts to balance requirements and resources through "smart sourcing."

The visits ended with a tour of the Global Network Operations and Security Center (GNOSC), and overview briefings by the Computer Emergency Response Team (CERT) and the Joint Task Force-Computer Network Operations (JTF-CNO). These visits are examples of the Director's effort to proactively engage senior customer leadership to develop delighted customers.

For additional information, contact Lt Col Bill McClure, CA3, (703) 882-2071, DSN 381.

Computing Services - Providing Configuration Management Support - By Beverly Griffith

DECC Detachment Montgomery
Maxwell AFB, Alabama

DISA's Computing Services provides configuration management services for several DoD programs. The Configuration Management (CM) office, located in Montgomery, AL, with liaisons in Washington D.C., is the recipient of the Director's Award for Computer/Computer Software Fields. CM strives to provide a high quality standard, repeatable configuration management process in a timely, low-cost manner. The office currently supports major programs such as Global Command and Control System (GCCS); Common Operating Environment (COE); Global Combat Support System (GCSS); Joint Defense Information Infrastructure Control System – Deployed (JDIICS-D); Composite Health Care System (CHCS-II); Systems Support Office-supported products such as Oracle, Tivoli, Managed Objects, Datametrics; and Enterprise Systems Management (ESM).

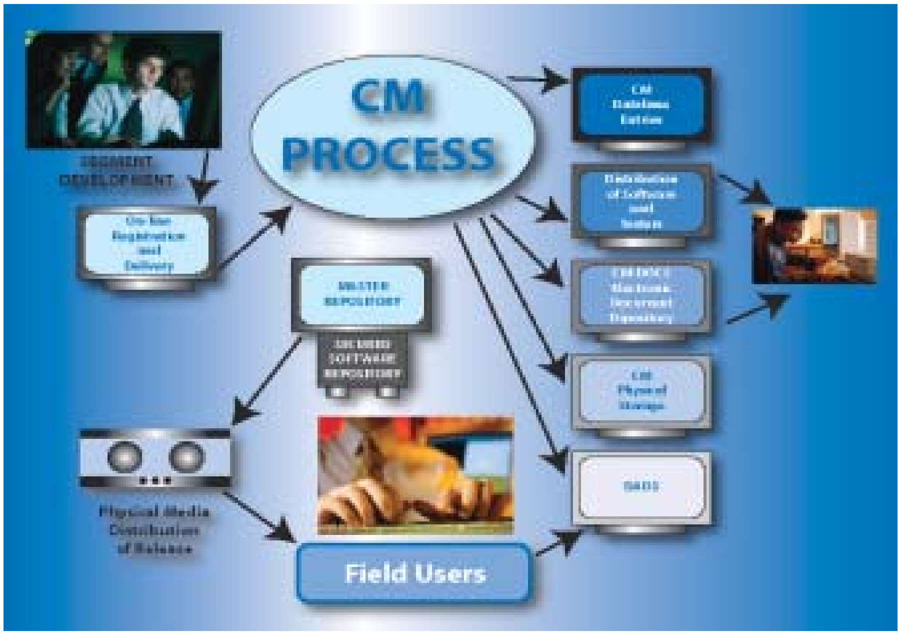
Program offices can realize major benefits by using this CM service. Some advantages include relieving the program office from handling software and/or documentation deliveries from their software developers available in the CM relational database. This database stores all post-development, life-cycle metadata regarding software, and documentation placed under CM control. Both physical (CDs, tapes, etc.), and encrypted electronic delivery capability from software developers are supported.

CM provides a tailorable, dynamic, frontend web capability to meet each program's requirements. These web pages are used by the software developers to register/track their software and documentation in the CM database; obtain CM numbers, schedule deliveries, request software, register ports and IDs; and enter problem reports/change requests. On-site liaison services are also provided.

Other services provided by CM include maintaining electronic repositories for both software and documentation, and supporting a physical library with all deliveries. Software is electronically distributed to multiple test sites and the documentation is available to the testers from the electronic repository. Data is also distributed electronically via the DII Asset Distribution System (DADS) using pull technology. In addition, DISA Montgomery maintains security certification and accreditation by the DISA Chief Information Officer (CIO). It has industry-certified network systems expertise, provides off-site storage, executes automated recovery procedures, and provides a 24x7 help desk.

These CM capabilities are provided by the DISA Center of Excellence for Configuration Management in Montgomery, which is staffed with a DISA team of experts who are dedicated to meeting customer needs in a timely, professional manner. In 2001, this center processed 7,180 delivery items, shipped more than 17,000 pieces of physical media, and placed 16,000 items on DADS for electronic distribution. Innovative improvements such as automated delivery capability, improved web interfaces, and automated CM number assignment have allowed the team to reduce delivery item processing time to less than 1.5 days. Because of the synergy that already exists with this group of professionals, expanding slightly to supporting more customers is a cost-effective method for meeting software and documentation configuration management needs.

For additional information, contact Beverly Griffith, CDTM2, at (334) 416-5422, DSN 596.

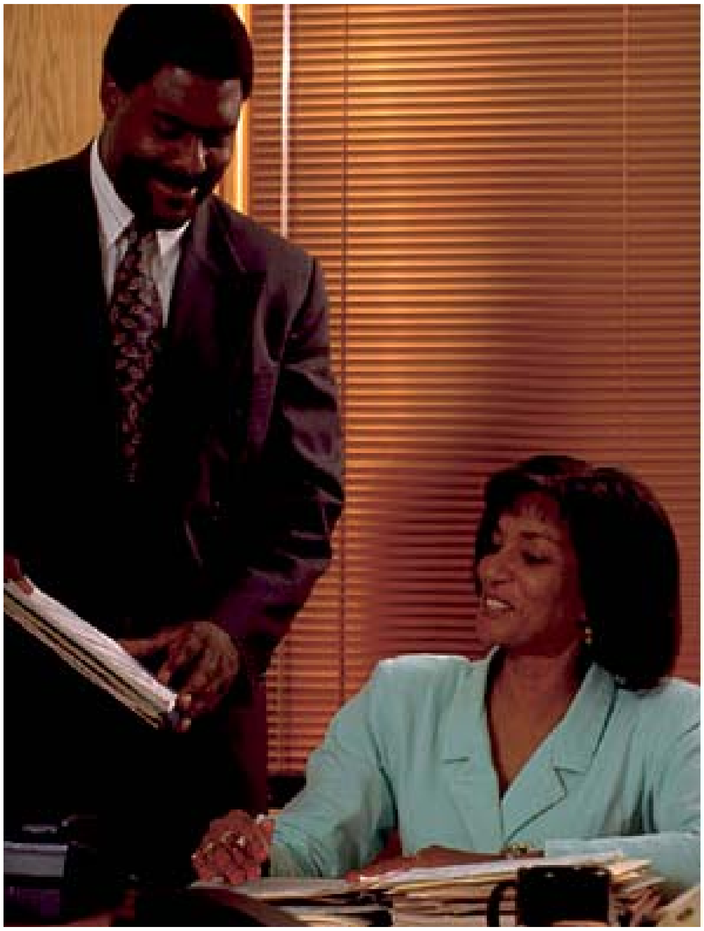

CM PROCESS
CM Database Entries
Segment Development
On-line Registration and Delivery
Distribution of Software and Testers
CM DOCS Electronic Document Repository
Master Repository
Secured Software Repository
CM Physical Storage
DADS
Physical Media Distribution of Release
Field Users

The CM process includes receiving software segments from developers, registering master repositories.

Got IT?

"A World of IT Acquisition Awaits You"
DISA's Acquisition Team (AQ)

By Joe Myers



The Directorate for Acquisition, Logistics, and Facilities (AQ) is the DISA world-class provider of creative, responsive, and best value information technology acquisition solutions.

AQ is where the customer needs them to be - "intheater". Providing global coverage, AQ has field offices strategically located in Hawaii, Alaska, Illinois, the National Capital Region, Germany, and Bahrain. Each field office has first-hand experience in anticipating and overcoming the unique challenges each theater of operations presents, and has become intimately knowledgeable of the mission and day-to-day, critical operational requirements of the customers. Coupled with their close proximity and partnership with industry, a triangle of success is created, focused on providing the best solution for the customer.

Whether planning an acquisition, writing statements of work, negotiating contracts, reducing prices, ordering products/services in a timely manner, ensuring service/product delivery, resolving billing disputes, or providing expert legal advice, AQ provides a comprehensive arsenal of acquisition services. AQ represents a global team of experienced professionals with a solid grasp on all facets of acquisition and the complexities of the information technology industry.

AQ offers solutions that cover the entire spectrum of information technology products and services. It rapidly acquires everything from networks, software, hardware, information security, operations and maintenance services, to total integrated business solutions. In pursuit of "best value to their customers," it has ready access to a variety of contracting solutions such as Basic Ordering Agreements, Blanket Purchase Agreements, Multiple-Award Contracts, Indefinite Delivery/Indefinite Quantity Contracts, GSA Schedules, Small Purchases, and other agency contracts.

Customers view AQ's solutions as fresh, flexible, forward-looking, and responsive. Innovative approaches such as 7-year contracts, award term, award fee, flexible labor categories, flexible partnerships, and "option less" contracts have yielded substantial benefits to the customer. AQ's streamlined processes and aggressive e-Business initiatives have provided an edge over traditional procurement options.

AQ is focused on customer service and satisfaction. Held in high esteem as an organizational value, AQ knows that customer satisfaction is earned through the deeds of individuals who take a vested interest in providing the best possible service. The individuals that make up the AQ family embody those beliefs.

Echoing the sentiments of the Director, AQ is committed to the warfighter and their other valued customers--the "Provider of Choice."

For additional information about AQ, contact Joe Myers at (618) 229-9392, DSN 779.

“Special Purpose” Gateway for Web Traffic - *By John Soles*

DISA’s Computing Services constructed a special purpose gateway hosting facility to ensure high availability of web servers that need to be accessible from the Internet even under conditions of distributed denial of service (DDoS) cyber attack. This special purpose gateway provides a solution to a growing e-commerce dilemma.

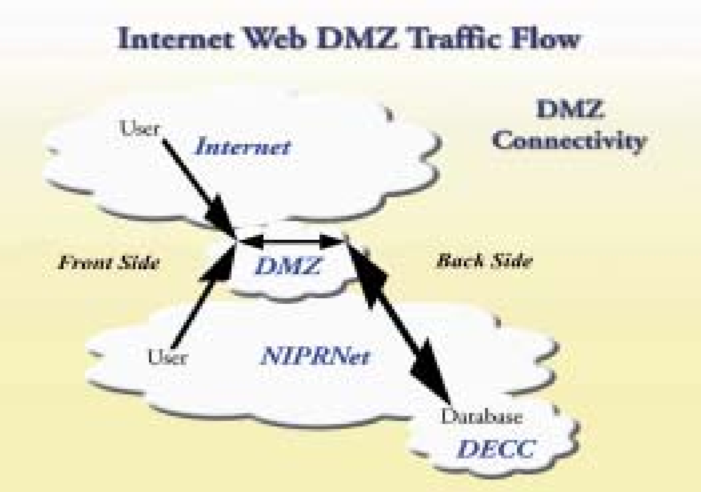
DoD E-Commerce

DoD has developed many online e-business websites that have assumed important infrastructure roles in daily logistics, personnel, finance, and transportation businesses. These sites must be available and accessible at all times by commercial trading partners for mission critical transactions. Many of these web sites have portals that get data from backend databases hosted at DECCs’.

DDoS Attacks on Web Servers

During the summer of 2001, the Internet was plagued by several DDoS attacks that targeted key Internet protocols like HTTP. The worst of these attacks was the Code Red worm. While relatively few DoD web servers were actually infected, the Code Red worm infected enough hosts (Internet-wide) to create a significant problem with bandwidth occupation. This in turn caused infected hosts to scan all other web servers on port 80 (the protocol port that the Code Red worm was attacking). The problem for e-commerce arises out of the fact that the Joint Task Force-Computer Network Operations (JTF-CNO) is forced to eliminate the attack by disallowing a service such as HTTP when it comes under attack. When port 80 was blocked, the effects of the attack were blunted, but the e-commerce sites were cut off from their critical customers’ points on the Internet.

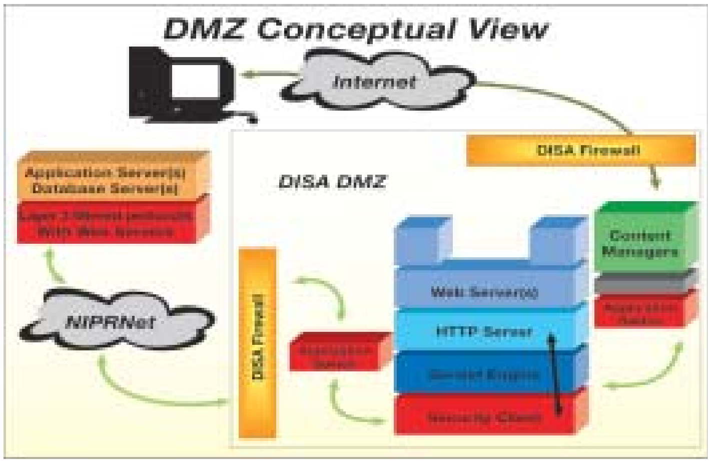
In order to eliminate this problem, DISA Computing Services looked at commercial best practices to provide a way to create web portals that would have constant availability for Internet use, without jeopardizing backend databases in particular, and the NIPRNet in general. The “DMZ Conceptual View” graph shows the general concept on how this configuration allows security to be optimized for attacks directed at ports 80 and 443. In addition, NIPRNet and its connected hosts are protected because web portals have restricted access to only legitimate back end hosts. The “Internet Web DMZ Traffic Flow” graph shows how and where the DoD Internet Web DMZ is placed in respect to the Internet, NIPRNet and DECCs. The front (Internet) side of the DMZ has extensive firewall and intrusion detection systems that allow the Internet or NIPRNet user to get to web servers through a very narrow suite of protocols. The backside of the DMZ only allows the web portals to access specific backend servers by IP address. Emphasis on the layered defense of NIPRNet is central to this design.



The DMZ site at DECC Columbus was completed in October 2001. This facility gives e-commerce managers a place to put their servers that will ensure continuous connectivity even when port 80 has to be blocked at the general purpose NIPRNet/ Internet gateways. Also, it allows NIPRNet access control and management to be significantly tightened.

Make it Distributed

Commercial best practices for high availability web portals dictate that the content should be replicated at multiple geographic locations so that cyber attack, network or server failure, or maintenance (scheduled or emergency) will not affect availability. This “assured computing” concept provides significantly better uptime than content that is hosted at a single facility. In addition to Columbus, DISA Computing Services is in the process of evaluating other locations as extensions to the DMZ at San Diego, Ogden, and San Antonio.



Customers Encouraged to Use DMZ

E-commerce users are encouraged to move their web portals to the DMZ in lieu of applying for GIG policy waivers from OSD for acquiring Internet connections. The GIG Waiver Board is increasingly inclined to deny these waiver applications because of their potential to compromise the NIPRNet. Potential customers should contact the DISA Computing Services business office. The point of contact is Karen Re, rek@ncr.disa.mil.

For additional information, contact John Soles, DISA Computing Services, Engineering and Communication Support Office, (703) 681-2696, DSN 761.

Senior Executive Account Manager (SEAM) Partnership Program

By Patricia Crabbe

DISA unveiled its new Customer Advocacy (CA) Directorate last October, which was created with the specific purpose of serving DISA's customers. In the aftermath of the September 11th tragedy, the importance of having such an organization became even more apparent.

Lieutenant General Harry Raduege, Director, DISA, insisted that the customer service initiatives be Agency-wide, which led to the formation of the Agency's Senior Executive Account Manager (SEAM) Partnership Program. The SEAM forges strategic partnerships and actively enhances the communication flow between DISA and its customers. A DISA Senior Executive or Flag Officer who works closely with a senior-level customer accomplishes this. How does the SEAM Program work?

The SEAM:

- Meets periodically with key customer senior leaders and maintains active communication via regular contact.
- Stays abreast of customers' strategic plans/priorities and keeps the DISA senior staff informed.
- Conveys DISA's evolving capabilities to customer leadership.
- Is committed to provide customer satisfaction and the timely resolution of customer issues.
- Works with DISA customer advocates for a specific organization to resolve issues.

Why do we need SEAMs?

SEAMs have a unique, executive perspective that enables the DISA team to fulfill more precisely the needs of its valued customers. As SEAMs, these senior leaders will provide the face-to-face interaction with the customers, which will in turn allow the agency to stay abreast of customers' issues and needs, and help resolve those issues quickly and to customers' satisfaction.

The SEAMs have valuable ties to each other, and can provide comprehensive information necessary for customer decision-making pertaining to the implementation of products and services, in addition to working together to provide timely solutions to customer complaints. While the SEAMs are creating a one-on-one partnership with their high-level customers, they are not working alone to provide solutions that will delight their customers. CA will provide support to the SEAM so that they do not become overwhelmed by the program's duties.

What are the Positive Benefits of a SEAM Partnership?

The SEAM partnership provides a clear path into DISA for customers to directly express their needs. This presents DISA with better information to provide the best and most appropriate products/services. The SEAM interaction also makes customers aware of new capabilities, and provides them with the information necessary for implementing new initiatives; it also supports the customer decision-making process. The SEAM/Customer Partnership enables issues to be raised to DISA senior leaders, so that a rapid resolution can be provided.

For additional information, contact Patricia Crabbe, CA1, (703) 882-0927, DSN 381.

DISA Morning Report

The following is a notional daily DISA Morning Report. The daily report provides a synopsis of the previous 24-hour DECC status for availability, packet loss, material release orders and communications. A description of open trouble tickets is also provided.

- The DISA Morning Report as of 0200 EDT/0700Z, 22 XXX 2002, is as follows:

- The NIPRNet AF portal is currently available on a continuous basis with no system outages or degradation of service to system components.

- Defense Security Assistance Management System (DSAMS) had no reportable outage(s).

- CHCS II status for the past 24 hours was green. Current status is green.

SITE	AVAILABILITY	PACKET LOSS	COMMENTS
DISA Montgomery	100.00%	0%	**COMMENTS**
Ft Eustis	100.00%	0%	**COMMENTS**
Langley AFB, VA	100.00%	0%	**COMMENTS**
Portsmouth, VA	100.00%	0%	**COMMENTS**
Seymour Johnson	100.00%	0%	**COMMENTS**

- Packet loss ≥ 3% is yellow. Packet loss ≥ 5% is red.

- DECC-D Montgomery CHCS II Network tickets are included at the end of section 4 “Reportable Network Issues”.

- Distribution Standard System (DSS) status is as follows:
  DECC Ogden DSS DII Report for period 21 XXX 03:00Z to 22 XXX 03:00Z
  Status for DECC Ogden for the last 24-hours is: green.

DEFENSE DISTRIBUTION DEPOT	ONLINE AVAILABILITY	MATERIAL RELEASE ORDER	COMMENT
San Joaquin, CA	100%	ON-TIME	GREEN
Oklahoma City, OK	100%	ON-TIME	GREEN
Red River, TX	100%	ON-TIME	GREEN
Corpus Christi, TX	100%	ON-TIME	GREEN
Barstow, CA	95%	ON-TIME	YELLOW
Puget Sound, WA	100%	ON-TIME	GREEN
Hill AFB, UT	100%	ON-TIME	GREEN
San Diego, CA	100%	ON-TIME	GREEN
Pearl Harbor, HI	100%	ON-TIME	GREEN
Yokosuka, Japan	100%	ON-TIME	GREEN

DECC Ogden ticket # 219014 - Columbus ticket # 174794. Seventy users at Base X were unable to access DSS using the NIPRNet because the circuit from Base X to Base Y was down. As a workaround the Base X users switched over to ISDN at 23:10 Zulu. Timeout: 02/21/2002 22:58 Zulu. Status: technicians at Columbus restored service at 02/22/02 0003 Zulu but the ticket remains in monitor status.

DECC-MECHANICSBURG DSS DII REPORT FOR PERIOD 21 XXX 01:00Z TO 22 XXX 01:00Z.
STATUS FOR DECC MECHANICSBURG FOR THE LAST 24 HOURS IS: GREEN

DEFENSE DISTRIBUTION DEPOT	ONLINE AVAILABILITY	MATERIAL RELEASE ORDER	COMMENT
Susquehanna, PA	100%	ON-TIME	GREEN
Richmond, VA	100%	ON-TIME	GREEN
Norfolk, VA	100%	ON-TIME	GREEN
Columbus, OH	100%	ON-TIME	GREEN
Tobyhanna, PA	95%	ON-TIME	YELLOW
Anniston, AL	100%	ON-TIME	GREEN
Warner Robins, GA	100%	ON-TIME	GREEN
Jacksonville, FL	100%	ON-TIME	GREEN
Cherry Point, NC	100%	ON-TIME	GREEN
Albany, GA	100%	ON-TIME	GREEN
Europe (Germany)	100%	ON-TIME	GREEN

The ATM has no critical and no high interest outage(s) during this reporting period.
The NIPRNet had two critical and four high interest outage(s) during this reporting period.

BG Carroll Pollett visits Iriduim facility and talks to customers and operations personnel at Wahiawa during his recent tour through the Pacific.

DEFENSE INFORMATION SYSTEMS AGENCY

CUSTOMER ADVOCACY

The Voice For The Warfighter

Principal Directorate for Customer Advocacy (CA)

Points of Contact List

Warfighter Support Division – CA2			
Bob Linthicum	Division Chief	703-882-1932	linthicr@ncr.disa.mil
Joe Re	OSD	703-882-2169	rej@ncr.disa.mil
Bill Austin	Intel Community	703-882-1942	austinw@ncr.disa.mil
MILDEP Support Division – CA3			
Lt Col Bill McClure	Division Chief/AF	703-882-2071	mcclurew@ncr.disa.mil
LTC Frank Higgins	Army	703-882-2175	higginsw@ncr.disa.mil
Tim Phillips	Navy/MC	703-882-2174	phillipt@ncr.disa.mil
Agency Support Division – CA4			
JoMarie Coburn	Division Chief	703-882-0711	coburnj@ncr.disa.mil
Mike Singleton	DoD/Fed Agencies	703-882-2173	singletm@ncr.disa.mil